The FBI's Carnivore: How Federal Agents May Be Viewing Your Personal E-Mail and Why There Is Nothing You Can Do About It

PETER J. GEORGITON*

Much controversy has arisen over the FBI's proposal to use an e-mail and Internet surveillance program, named "Carnivore," to assist its law enforcement efforts on the Information Superhighway. In this note, the author examines how Carnivore operates and its implications for individuals' privacy rights under the Fourth Amendment and the Electronic Communications Privacy Act of 1986 (ECPA). The author concludes that the current state of constitutional and statutory law governing electronic surveillance indicates that the FBI can utilize Carnivore to conduct a wide range of intrusive searches with little or no legal justification. Carnivore's ability to retrieve more than mere e-mail messages of suspects, the FBI's checkered past on privacy issues, and the lack of judicial oversight make the potential for abuse of Carnivore great. As a result, Congress must take a hard look at both the ECPA and Carnivore to prevent law enforcement agencies from using Carnivore to peer into our personal e-mails and Internet usage.

Whether he wrote DOWN WITH BIG BROTHER, or whether he refrained from writing it, made no difference. . . . The Thought Police would get him just the same. He had committed—would still have committed, even if he had never set pen to paper—the essential crime that contained all others in itself. Thoughtcrime, they called it. Thoughtcrime was not a thing that could be concealed forever. You might dodge successfully for a while, even for years, but sooner or later they were bound to get you.[**]

I. INTRODUCTION

The Federal Bureau of Investigation (FBI) and the Justice Department have recently come under fire after a revelation by *The Wall Street Journal* of the existence of Carnivore, a computer software program capable of searching

---

* B.A., Wittenberg University, 1999; J.D., The Ohio State University, 2002 (expected). I would like to thank Attorney Michael H. Gertner, a good friend and mentor, for bringing the issue of Carnivore to my attention. Without his healthy skepticism about the ability of law enforcement agencies to simultaneously deploy new search technologies and protect individuals' civil liberties, this note would have never come into existence. Special thanks to Professor Peter P. Swire, who graciously reviewed this note and offered helpful comments and criticisms. I would also like to extend thanks to the staff of the *Ohio State Law Journal* for their hard work and dedication in editorial process. Finally, I would like to dedicate this note to Elizabeth Vanlier, whose love and support helped sustain me while I was writing this note.

** GEORGE ORWELL, 1984 19 (Plume Books 1983) (1949).

countless numbers of e-mails in order to find potential terrorists, pedophiles, hackers, and other persons using the information superhighway to commit crimes.[1] Carnivore operates as a "packet sniffer," catching bits and pieces of data sent from one Internet user to another and then reassembling them for the FBI to examine.[2] Tests have shown Carnivore to be highly effective at filtering e-mail messages for criminal content, and it is this high rate of effectiveness that raises serious privacy concerns.[3] Of paramount concern is that the FBI might unleash Carnivore on thousands of unsuspecting users of the Internet in an attempt to find the criminals among us, and, in the process, examine the content of personal e-mails and invade our privacy. The FBI has tried to dispel privacy concerns regarding Carnivore, contending that a warrant is required before any agent can conduct a search, and that any unauthorized searches would result in criminal and civil liability for the agent.[4]

---

[1] *See* Neil King, Jr. & Ted Bridis, *FBI's Wiretaps To Scan E-Mail Spark Concern*, WALL ST. J., July 11, 2000, at A3. The FBI has recently backed away from likening its surveillance equipment to flesh eating animals as "Carnivore" is now simply referred to as "DCS-100." Larry Kahaner, *Hungry for Your E-Mail – IT Managers and ISPs Fear FBI E-Mail Monitoring Device Will Hurt Systems and Invade Privacy*, INFORMATIONWEEK, Apr. 23, 2001, at 59. For ease of recognition, the term "Carnivore" will be used throughout this note to refer to the FBI's e-mail and Internet surveillance tool.

[2] *See* Md. Qaisar Alam, *E-Mail Surveillance: Carnivore Cornered*, COMPUTERS TODAY, Oct. 31, 2000, at 48. "Packet sniffer" refers to Carnivore's form of searching information sent out over the Internet. *Id.* When sent from a user's computer to another computer on the Internet, web info, e-mail, and other Internet data are split up into individual parts or "packets." *Id.* The destination computers, upon receiving the packets, reassemble them and display them to the other user. *Id.* Carnivore intercepts each of the individual packets as they pass over the Internet, "sniffing" them to determine whether or not they contain objectionable material. *Id.* Packets that trigger Carnivore's search criteria are then copied onto Carnivore's hard drive. *Id.* The FBI later reassembles the packets to find out the contents of the data. *Id.*

[3] Although Carnivore is championed by the FBI as a tool to be used solely for searching e-mails, an independent report by the Illinois Institute of Technology (commissioned at the request of the Department of Justice) revealed that the program is capable of "view[ing] the content of e-mail messages, HTTP [web] pages, FTP sessions, etc." Stephen P. Smith et al., *Independent Review of the Carnivore System* ix (Dec. 8, 2000) [hereinafter *Carnivore Independent Review*], *available at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf.

[4] In a series of hearings during Summer 2000 on Capitol Hill, the FBI stated that all searches must be conducted pursuant to the Electronic Communications Privacy Act of 1986 (ECPA). Thus, before a Carnivore search could begin, the FBI must obtain a court-ordered warrant supported by probable cause, and agents who go beyond the warrant's search parameters would be subject to criminal and civil penalties under the Act. *See* Donald M. Kerr, *Statement for the Record of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation, on Carnivore Diagnostic Tool, Before the United States Senate, The Committee on the Judiciary, Washington, D.C., at* http://www.fbi.gov/congress/congress00/kerr090600.htm (Sept. 6, 2000). The gist of Mr. Kerr's statement to Congress was that the ECPA provides sufficient protections to prevent Carnivore from being abused. Kerr emphasized that "[u]nder this law, the FBI cannot, and does not, 'snoop,'" because warrants issued under the ECPA must be sufficiently particular and state "the offenses being committed,

Comforting as the FBI's assurances may sound, the current status of the constitutional and statutory law governing electronic surveillance indicates that the FBI is free to conduct a wide range of intrusive searches with Carnivore. This note will examine the overlooked privacy implications of Carnivore's uses. In particular, this note will focus on the fact that, if used in the limited capacity that the FBI publicly intends, Carnivore is perfectly legal under the constitutional and federal statutory framework in place today. However, Carnivore's capacity for searching through more than just e-mail of known criminal suspects, coupled with the FBI's checkered past on privacy issues and the lack of judicial oversight make the potential for abuse great. As a result, Congress will need to take a hard look at both the Electronic Communications Privacy Act of 1986 (ECPA) and Carnivore and add new protections to prevent Carnivore from becoming the ever-peering eye of the government.

Part II of this note will examine Carnivore's background, why the FBI determined that it was necessary, and how Carnivore operates during a typical search. Part III will examine the constitutional framework governing searches involving Carnivore. It will ask whether e-mail users have a reasonable expectation of privacy in their mail such as to require probable cause to justify a search. It will also demonstrate that this expectation of privacy may not extend to all searches conducted with Carnivore, leaving the FBI free to conduct searches without probable cause. Part IV of this note will examine the constitutional requirement of particularity in warrants for seizure of documents and explore this requirement's interaction with searches of e-mail messages using Carnivore. Part V will examine Congress' response to perceived weaknesses in the constitutional doctrine in the Electronic Communications Privacy Act of 1986 (ECPA) and demonstrate how the ECPA is insufficient to protect e-mail users from unauthorized searches by the FBI. Part VI will discuss how the lack of neutral, third-party oversight of the FBI's use of Carnivore, coupled with the FBI's past history of abuse, makes it possible for the FBI to use Carnivore to "snoop" around in our personal e-mails. Finally, Part VII will discuss some potential remedies Congress could use to protect the public from invasions of privacy by devices like Carnivore.

II. BACKGROUND

A. *Why is Carnivore Necessary?*

According to the FBI, the growth of the Internet over the last five years has led to increased use of the "Information Superhighway" by "terrorists, spies,

---

the communications facility regarding which the subject's communications are to be intercepted, a description of the types of conversations to be intercepted, and the identities of the persons committing the offenses and anticipated to be intercepted." *Id.*

hackers, and dangerous criminals . . . to carry out their heinous acts."[5] In a statement before the Senate Judiciary Committee, Donald M. Kerr, Assistant Director of the FBI's Laboratory Division, cited Central Intelligence Agency (CIA) information that various foreign and domestic terrorist groups use e-mail and other Internet resources to further their causes.[6] In addition, Kerr referred to other concerns of national and domestic security such as espionage, "'information warfare' by foreign militaries against [the United States'] critical infrastructures," sexual exploitation of children, and serious fraud.[7] In the FBI's view, Carnivore, by automatically filtering and intercepting e-mails of suspects listed in warrants, provides an efficient way to gather incriminating evidence without offending the Fourth Amendment or the federal electronic privacy laws.[8]

B. *How Carnivore Works*

At first glance, the Carnivore program does not appear any different from a program one might run on one's home, Windows-based computer. The visual set up is very familiar: the program is accessed through the click of an icon, and the main program has an active window with the traditional "minimize," "maximize," and "close" buttons at the upper right hand corner of the screen. But the similarities end with the title screen, which immediately foreshadows the powerful nature of this program by displaying a small graphic of blood-soaked teeth "chomping" on a meal of binary numbers.[9] Compounding these differences is the fact that the computer from which the Carnivore program is operated is merely a workstation connected via a telephone network to the main Carnivore computer located at the Internet Service Provider's (ISP's) headquarters. Carnivore has no monitor or keyboard, and the computer it uses is enclosed in a locked, black box connected to the outside world only through a direct connection

---

[5] *Id.*

[6] *Id.*

[7] *Id.* Some of the examples cited by Kerr included CIA information that terrorist groups such as Hezbollah, HAMAS, and Osama Bin Laden's Qa'ida group were using computer files and e-mail for their terrorist planning. Kerr also stated that since countries know that they cannot beat the U.S. with their military forces, they are instead targeting "our growing dependence on information technology in government and commercial operations." Particularly interesting was Kerr's citing of a Russian official's comments that "an attack on a national infrastructure could, 'by virtue of its catastrophic consequences, completely overlap with the use of [weapons] of mass destruction.'" *Id.*

[8] *Id.* The FBI contends that protection of individuals' constitutional rights was what it had in mind in creating Carnivore, as many commercial "sniffers" or search tools "collect either too much information, such as collecting all of the information regarding a given criminal subject's account, or, alternatively, fail to collect the authorized information at all." *Id.*

[9] *See* Electronic Privacy Information Center, *Carnivore Test Procedure Special Service Pack Update*, *at* http://www.epic.org/privacy/carnivore/test1.html (Sept. 27, 2000) (containing Carnivore materials requested by the Electronic Privacy Information Center under the Freedom of Information Act).

to the ISP's mainframe and a phone line to the FBI offices.[10] To operate Carnivore, the FBI agent inputs the search ("filter") criteria, which can include particular Internet ports, specific Internet Protocol (IP) addresses,[11] Simple Mail Transfer Protocol (SMTP) and Post Office Protocol 3 (POP3) addresses,[12] individual usernames for a particular Internet or e-mail account, and specific text strings contained in e-mails.[13]

Once the filter criteria have been established, the Carnivore program is run from the FBI's office, and the computer located next to the ISP's server begins to search for e-mail that meet the criteria. When an Internet user sends e-mail to another location on the Internet, it is typically broken into individual "packets."[14] These packets may travel different routes to the final destination where, upon arrival, they are assembled into a whole e-mail message again.[15] Carnivore acts as a "packet sniffer" by intercepting packets that meet the FBI's pre-established search criteria.[16] The intercepted packets are saved on a Jazz disk (a special magnetic disk that can hold two gigabytes of information, or enough information to fill 1,400 high density floppy disks),[17] and then retrieved by an FBI agent who travels to the ISP's headquarters, unlocks Carnivore, and removes the disk.[18]

The packets received by the FBI are unusable unless they are reassembled and decrypted. Programs named "Packeteer" and "Coolminer" take the

---

[10] Many privacy advocates and ISPs have been concerned about Carnivore's mysterious nature. Because it is located in a locked, black box, even the ISP cannot be sure what Carnivore is retrieving. Ultimately, only the FBI knows what Internet traffic is pulled aside by Carnivore. D. Ian Hopper, *Critics Fret About FBI's Interceptor For E-Mail*, PLAIN DEALER (Cleveland), July 12, 2000, at 11A.

[11] Every web site and computer connected with the Internet has a unique Internet Protocol address, which consists of a series of numbers. For example, The Ohio State University's IP address for its web page is "128.146.214.28". By constraining Carnivore's search to a particular IP address, this would mean that only data from that IP address would be collected.

[12] Most e-mail services have incoming (POP3) and outgoing (SMTP) mail servers. Each of these servers in return has a unique address, which can be used to retrieve e-mail from a remote computer using mail applications such as Microsoft Outlook or Eudora. The address for The Ohio State University's POP3 student mail server, for example, is "pop.service.ohio-state.edu".

[13] *Carnivore Independent Review*, *supra* note 3, at xii. Using the text-filtering feature of Carnivore, an Agent could type specific text strings such as "bomb" and "embassy" to have Carnivore intercept all e-mails containing those words. *Id.*

[14] Alam, *supra* note 2, at 48.

[15] *Id.*

[16] *Id.*; *Carnivore Independent Report*, *supra* note 3, at ix.

[17] The Illinois Institute of Technology Research Institute's report on Carnivore states that, while the information is stored on a retrievable Jazz disk, there is no technical barrier preventing information intercepted by Carnivore from being stored on a hard disk drive, which would greatly increase the amount of material Carnivore would be able to retrieve and subsequently store. *See Carnivore Independent Report*, *supra* note 3, at 3-15.

[18] *Id.* at 3-5.

information gathered by Carnivore and reconfigure it into usable data.[19] If the e-mail is encrypted to make it unreadable, other programming must be utilized for decryption.[20]

III. E-MAIL AND THE REASONABLE EXPECTATION OF PRIVACY

Carnivore's use by the FBI immediately raises concerns about potential infringement of individuals' privacy rights. There are two principle protection mechanisms already in place that limit the FBI's ability to use Carnivore: the Fourth Amendment and its case law, and the ECPA. These protections ensure that, at a minimum, the FBI must obtain a warrant if it wishes to search the contents of e-mail or a court order if it merely wishes to use Carnivore to obtain e-mail addresses. Questions remain, however, as to the effectiveness of these limitations in preventing abuse of Carnivore, especially since they were created before the explosion of Internet and e-mail usage. What is clear, however, is that the current constitutional and statutory framework grants substantial protection from the most intrusive searches of e-mail by Carnivore, but it has many loopholes that leave the public unprotected from less intrusive searches.

A. *The Constitutional Framework: the Fourth Amendment's Protection from Unreasonable Searches and Seizures*

Along with the First Amendment's protection of freedom of speech and religion, the Third Amendment's protection of freedom from quartering of soldiers, and the Fifth Amendment's protection from self-incrimination, the Fourth Amendment is part of what one author describes as a dominant theme in constitutional law: protecting the privacy rights of the individual from intrusion by the federal government.[21] The Fourth Amendment states that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation and particularly describing the place to be searched, and the persons or things to be seized.[22]

Warrantless searches are presumptively unreasonable, and in order for law enforcement agencies such as the FBI to search one's home, there must be a warrant, particularly describing the places and things to be searched, and supported by evidence tending to show probable cause that the evidence to be

---

[19] *Carnivore Independent Report*, *supra* note 3, at ix.

[20] Alam, *supra* note 2, at 48.

[21] Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877, 884 (2000).

[22] U.S. CONST. amend. IV.

searched and/or seized will establish the existence of a crime.[23] The requirement of a warrant prevents the police from rummaging through individuals' homes and personal effects unless a neutral magistrate makes a determination that there is probable cause to justify the intrusion.[24]

But in order for the Fourth Amendment's protections to apply, the government activity must first qualify as a search or seizure. One of the first United States Supreme Court cases to deal with the issue of whether the interception of communications constitutes a "search" for Fourth Amendment purposes was *Olmstead v. United States*.[25] In *Olmstead*, the petitioner tried to suppress evidence retrieved via a telephone tap placed outside of his house because it had been obtained without a warrant. Writing for the majority, Chief Justice Taft recognized that a person has privacy rights under the Fourth Amendment in certain places, such as the home, but nonetheless held that the phone tap did not constitute a search and therefore did not require a warrant because the tap was placed *outside* of the home.[26]

This view of personal rights under the Fourth Amendment held firm until the Court revisited the issue of phone taps in *Katz v. United States*.[27] In *Katz*, the defendant was charged with placing bets over the phone in violation of federal law. The government based its case against Katz in part on conversations made by him in a public telephone booth, which had an electronic listening and recording device attached to it by the FBI. Though the government contended that taps of public phone booths did not violate one's right to privacy or constitute a search, the Court dramatically reformulated privacy doctrine by holding that the "Fourth Amendment protects people, not places."[28] The Court noted that, despite the fact that phone booths are made of clear glass and are located in public, a person who uses the telephone expects their conversations to remain private.[29]

---

[23] Berger v. New York, 388 U.S. 41, 58 (1967).

[24] *See* Johnson v. United States, 333 U.S. 10, 14 (1948).

[25] 277 U.S. 438 (1928).

[26] *Id.* at 465. Chief Justice Taft stated:

> The [Fourth A]mendment does not forbid what was done here [installing a phone tap outside of a house]. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants . . . . [T]he intervening wires are not part of his house or office any more than are highways along which they are stretched.

Id. at 464.

[27] 389 U.S. 347 (1967).

[28] *Id.* at 351.

[29] *Id.* at 352. The Court noted that at the time of the decision, the telephone had become accepted as a vehicle of private conversation:

> No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be

Justice Harlan's concurrence in *Katz* set up the two-pronged test used by the Court today in determining whether government activity constitutes a search and implicates Fourth Amendment privacy interests. The first prong is a subjective test: whether the person has an actual expectation of privacy. The second prong is objective: whether society is prepared to accept the person's expectation of privacy as reasonable.[30] Taken together, the question asked is whether the person who is being observed has a reasonable expectation of privacy.

While it provides much comfort to know that the FBI must have a warrant before it can search certain things in which one has a reasonable expectation of privacy, what exactly constitutes a "reasonable expectation of privacy" is often unclear. The easy cases deal with situations involving face-to-face searches of our homes or searches involving established technology, such as when authorities listen in on phone calls using phone taps. However, what about e-mail? Can a user of an e-mail service have a "reasonable expectation of privacy" in the contents of his or her e-mail so that the FBI must first flash a warrant at a terrified, twenty-something computer tech at America Online (AOL) before it starts sorting through users' love letters? The answer is that it depends on what type of e-mail service one is using and on how much information agencies like the FBI want.

1. *Searches of Home E-Mail*

The type of e-mail most near and dear to people's privacy concerns is their home e-mail accounts, which are utilized everyday for various types of communications, and which most people would probably expect to remain private. Surprisingly, the Supreme Court has not had occasion to address whether there is a reasonable expectation of privacy in our personal home e-mail accounts, and there is little case law directed to the issue as well. But overall, the courts that have addressed the issue have found that people do indeed have a reasonable expectation of privacy in their e-mail communications made from their personal accounts.[31]

---

broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

Id. This quote parallels the current state of e-mail, for as our dependence on it has grown, our expectation that our e-mail communications will remain private has increased.

[30] *Id.* at 361 (Harlan, J., concurring). Applying the test, Justice Harlan states that it is natural for there to be times where we expect our phone calls made from a public phone booth to remain private. Even though the phone booth is located in public, as a society we recognize that at times "it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable." *Id.*

[31] In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA) to extend existing wiretap protections to electronic communications, such as e-mail. Though there had not been a judicial determination of whether there is a reasonable expectation of privacy in e-mail at that point, the House Judiciary Committee's report suggested that this would be the course the courts would follow. *See* H.R. REP. NO. 99-647, at 17 (1986).

The leading case addressing the issue of privacy in personal e-mail accounts was decided by the United States Court of Appeals for the Armed Forces in *United States v. Maxwell*,[32] in which an AOL user reported to the press that he had received child pornography through the Internet service. In response to the complaint, AOL notified the FBI, which subsequently searched the account files of the defendant, an Air Force colonel, on the AOL central computers. The search included his personal e-mails and recovered pornographic materials. Though the FBI had obtained a warrant to search the files at AOL, there were many indications that the search in fact had exceeded the authority of the warrant.[33]

The court was thus confronted with the issue of whether the defendant had standing to contest the search in the first place by demonstrating that he had a reasonable expectation of privacy in his AOL e-mail account.[34] At the outset, the court noted the difference between e-mails accessed with the AOL service and simple messages posted on the Internet, the former of which "are afforded more privacy . . . because they are privately stored for retrieval on AOL's centralized and privately-owned computer bank . . . ."[35] In addition, the court relied upon testimony of AOL officials who stated that AOL, as a matter of policy, would not read or disclose its members' e-mails to anyone, unless authorized by the user or served with a court order.[36] In light of this policy and the private nature of e-mails

---

[32] 45 M.J. 406, 412 (Ct. App. A.F. 1996). The user in this case had originally reported the receipt of child pornography to his local law enforcement officials, but after receiving no assistance, subsequently took his case to the press.

[33] *Id.* at 416. The court noted that AOL employees—and not FBI agents—conducted the search, the warrant had "at least 20 or more errors," the seizure "exceeded the plain language of the warrant," and AOL did not rely on the warrant in designing search programs to search its files. *Id.*

[34] *Id.* Sensing the new ground in privacy law this case was treading, the court commented:

> [P]ersonal computers, hooked up to large networks, are so widely used that the scope of Fourth Amendment core concepts of 'privacy' as applied to them must be reexamined. Consequently, this opinion and the ones surely to follow will affect each one of us who has logged onto the "information superhighway."

Id. at 410.

[35] *Id.* at 417.

[36] *Id.* Indeed, the prevalence of similar privacy policies at other Internet Service Providers enhances users' expectation of privacy in their e-mail communications. CompuServe explicitly states in its Terms of Use agreement that it will not read users' e-mails: "You are solely responsible for your e-mail . . . and acknowledge that CompuServe acts as a passive conduit for the transmission of such data." However, CompuServe alerts users that it is "legally obligated to provide member e-mail information (including actual e-mail messages . . .) if served with proper legal documentation" by law enforcement authorities under the provisions of the ECPA. CompuServe USA, *CompuServe Privacy Policy*, *at* http://www.compuserve.com/login/LoginTermsofService.asp (Sep. 30, 2001). Other e-mail services, such as Microsoft's Hotmail, guarantee privacy of user information, but do not explicitly guarantee privacy of the contents of e-mails:

> MSN is committed to protecting your privacy and developing technology that gives you

sent using AOL, the court concluded that the defendant "possessed a reasonable expectation of privacy" in his e-mails.[37]

However, the court recognized that the "type of e-mail involved and the intended recipient" could limit this reasonable expectation of privacy.[38] First, when someone sends out e-mail, the reasonableness of his or her privacy expectation begins to decrease. For example, if the message is posted in a chat room or otherwise transmitted in an open fashion, one cannot have a reasonable expectation of privacy. Also, it is not reasonable to assume that the contents of the e-mail message will remain private once received by the intended recipient. With this line of reasoning, the court analogized e-mail to postal mail: Someone who sends a letter sealed in an envelope can reasonably expect it to remain private until it is received by the third party, but she bears the risk that the third party might disclose the letter's contents to the authorities.[39] One sending an e-mail using an AOL account, the court reasoned, does not enjoy a reasonable expectation to total privacy of the message; reasonable expectations instead are limited to the belief that "police officials will not intercept the transmission without probable cause and a search warrant."[40]

Other cases have reaffirmed *Maxwell*'s requirement of a warrant for searches of e-mail. The Court of Appeals for the Armed Forces in *United States v. Monroe*[41] found that users of a government e-mail system had a reasonable expectation that law enforcement officers would not intercept their messages even though there was specific notice that the system administrator was monitoring the e-mail.[42] Though not confronting the issue directly, other courts have assumed in

---

> the most powerful and safe online experience. . . . Microsoft and MSN are licensees of the TRUSTe Privacy Program. TRUSTe is an independent, non-profit organization whose mission is to build trust and confidence in the Internet. . . . [T]his website has agreed . . . to have its privacy practices reviewed for compliance by TRUSTe.

Microsoft Network, *MSN Hotmail Privacy Statement*, *at* http://www.hotmail.com/help/legal/privacy.htm (last modified June 2000).

[37] *Maxwell*, 45 M.J. at 417.

[38] *Id.* at 418–19.

[39] *Id.* The court also found that the same expectation of privacy existed for telephone calls, as we expect our conversations to remain private and not be intercepted by the police, but we bear the risk that the person on the other end of the line will squeal to the police after hanging up. *Id.* at 418.

[40] *Id.*

[41] 52 M.J. 326 (Ct. App. A.F. 2000).

[42] *Id.* at 330. In line with its earlier decision in *Maxwell*, however, the court held that when one has notice that the system administrator is monitoring e-mail, there is no reasonable expectation that the administrator will not turn the e-mail over to the authorities. *Id.* The United States Court of Appeals for the Fourth Circuit considered a similar scenario, where an employee for the CIA was prosecuted after a remote search of his office computer turned up child pornography. United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000). Since he had been informed that it was agency policy to "audit, inspect, and/or monitor" Internet use by employees, he enjoyed no reasonable expectation that the agency would not search his

dicta that users have reasonable expectations of privacy in their e-mail messages.[43]

2. *Addressing, Routing, and Signaling Information and the Pen Register Problem*

As these cases suggest, it is not unreasonable for someone to assume that their e-mails will remain private and will not be intercepted by the FBI using Carnivore without first obtaining a warrant from a neutral magistrate. While this protection is comforting, the FBI can use Carnivore to keep track of routing and addressing information of e-mails (incoming and outgoing) and websites visited by individuals using Carnivore's pen register/trap and trace mode.[44] Under current federal law, not only is a warrant *not* required for interception of addressing information, but also the ECPA's provisions regulating pen register/trap and trace devices are inadequate for protecting Internet users' privacy interests.

In their traditional use, law enforcement officials utilized pen registers and trap and trace devices for telephone lines, recording the phone number of all outgoing and incoming calls made on a suspect's line. Like a telephone tap, a pen register or trap and trace device requires monitoring of a telephone line, but, as the Supreme Court has held in *Smith v. Maryland*, does not require a warrant where none of the contents of the telephone communication are revealed.[45] However, pen registers and trap and trace devices are governed under the ECPA, where agents are required to apply for a court order upon a showing that "the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[46]

The same requirements apply to pen register/trap and trace searches of addressing and routing information using devices like Carnivore.[47] Similar to the

---

computer and turn over the materials to the authorities. *Id.*

[43] *See* Dunlap v. County of Inyo, Nos. 96-15207, 96-15294, 96-15915, 1997 U.S. App. LEXIS 19249, at *9 (9th Cir. July 23, 1997) ("Cellular telephones and electronic mail are both technologies of questionable privacy, but we nonetheless reasonably expect privacy in our cell phones and email [sic] messages."); United States v. Lamb, 945 F. Supp. 441, 455 n.9 (N.D.N.Y. 1996) (assuming that the defendant had a reasonable expectation of privacy in the files located in his AOL account).

[44] *See Carnivore Independent Review*, *supra* note 3, at 3-21 (generally describing test of Carnivore's e-mail addressing information collection procedures).

[45] *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding that there is no reasonable expectation of privacy regarding the numbers defendant dialed on his phone, as "all phone users realize that they must 'convey' phone numbers to the telephone company").

[46] 18 U.S.C. § 3122(b)(2) (1994).

[47] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 216(c)(2), 115 Stat. 272 (extending the definition of Pen Register in 18 U.S.C. § 3127(3) (1994) to include "dialing, routing, addressing, or signaling information transmitted by an

pen register, Carnivore can be set to retrieve only information concerning where an outgoing e-mail was sent, where an incoming e-mail was sent from, and the e-mail address itself.[48] The FBI contends that, consistent with *Smith*, they can retrieve this information without need for a warrant.[49] Privacy experts have cried foul, however, contending that an e-mail address reveals much more than a simple phone number.[50] Whether the FBI will require a warrant to conduct a pen register search with Carnivore will depend on whether e-mail users have a reasonable expectation of privacy not only to the contents of their e-mail but also to the addressing information. *Smith* suggests that the FBI does not need a warrant in order to get the addressing information from someone's e-mail account, and equally troubling is the fact that the provisions of the ECPA require only *minimal* justification for searches of addressing and routing information, even though this information may reveal considerable details about an individual.

The Supreme Court considered the Fourth Amendment issues surrounding

---

by an instrument or facility from which a wire or electronic communication is transmitted." However, devices which intercept "the contents of any communication" are expressly excluded from the definition); *id.* § 216(c)(3) (extending definition of Trap and Trace Device in 18 U.S.C. § 3127(1) (1994) to include "dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication").

[48] *See Carnivore Independent Review*, *supra* note 3, at 3-2.

[49] *See Kerr*, *supra* note 4.

[50] *See* Kevin Butler, *Is Big Brother Surfing the Internet?: FBI's 'Carnivore' Raises Privacy Issue*, INVESTOR'S BUS. DAILY, Aug. 9, 2000, at A22 (quoting privacy advocates' complaints that allowing pen register/trap and trace searches of Internet addressing information "goes far beyond what the Supreme Court OK'd in 1979 [with the *Smith* decision]"). Philip L. Gordon, an attorney at the Privacy Foundation, commented in *The Wall Street Journal* that Carnivore's capture of e-mail addressing information is "clearly different" from pen registers. Ted Bridis, *FBI's E-Mail Suggest Divisions On Legality of Web Surveillance*, WALL ST. J., Dec. 7, 2000, at B9. Specifically, experts have commented that "the record of a phone call placed to a certain number won't necessarily identify the people who talked, but e-mail sent to a particular address allows police to derive identities with greater precision." *Id.* Even the FBI's own internal agents initially questioned the legality of the pen register/e-mail address capture feature of Carnivore, but the FBI later attributed the division to the "inexperience of some bureau field offices dealing with the latest technology tools and policy questions they raise." *Id.*

Critics who are concerned that Carnivore's pen mode will reveal more than just an e-mail address may be on the right track. The Illinois Institute of Technology Research Institute found that there were cases of "potential over-collection in pen mode." *See* Steven M. Bellovin et al., *Comments on the Carnivore System Technical Review*, *at* http://www.crypto.com/papers/carnivore_report_comments.html (Dec. 3, 2000). Under some circumstances, even though Carnivore is programmed only to collect an address, it may actually retrieve an entire packet, which would contain content. *Id.* The report also noted that in pen mode, Carnivore could determine the length of various communications, thus allowing web "traffic analysis" and identification of the web pages a user was visiting. *Id.*

Congress has recognized the distinction between telephone numbers and e-mail addresses, stating that it was "[r]ecogniz[ed] that transactional records from on-line communication systems reveal more than telephone toll records." S. REP. NO. 103-402, at 31 (1994).

pen registers in *Smith v. Maryland*.[51] In *Smith*, the local police had attached a pen register to the defendant's telephone line to determine whether he had robbed and subsequently placed threatening calls to a woman. The pen register revealed that the defendant had indeed called the woman's home, and on that basis the police obtained a warrant to search his home. The defendant challenged the search warrant, arguing that the police's use of the pen register was a search within the meaning of the Fourth Amendment and thus required a warrant. Applying the analysis utilized in *Katz*, the Court held that the defendant had no reasonable expectation of privacy in the numbers he dialed on his phone.[52] In reaching its decision, the Court was quick to distinguish the pen register used in the case from the telephone wiretap used in *Katz*, noting that "pen registers do not acquire the *contents* of communications."[53] The Court reasoned that the defendant had no legitimate expectation of privacy in the numbers he dialed on his phone because "all telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." [54] Additionally, everyone who utilizes phone services, according to the Court, realizes that companies keep track of phone numbers for billing and long distance purposes, as well as to respond to annoying and obscene calls.[55] Furthermore, according to the Court, even if the defendant did have a valid expectation of privacy, it was not an expectation that society would view as reasonable, because he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[56]

No court has taken the inferential step and applied the *Smith* rule regarding the apprehension of telephone numbers to the apprehension of e-mail addresses through electronic surveillance. However, lower courts, while not explicitly considering whether a person has a reasonable expectation of privacy in the addressing information for their e-mail, have been largely reluctant to consider anything beyond the content of electronic communications in their *Katz* (reasonable expectation of privacy) analysis. For example, in *United States v. Hambrick*,[57] the Fourth Circuit Court of Appeals expressly construed the *Katz* rule to apply only to the content of e-mails, thus implicitly excluding e-mail addresses from its protection.[58] *Hambrick* dealt with an Internet user's expectation

---

[51] 442 U.S. 735 (1979).

[52] *Id.* at 742.

[53] *Id.* at 741.

[54] *Id.* at 742.

[55] *Id.*

[56] *Id.* at 744. The Court cited *Katz* and other cases for the proposition that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743–44.

[57] No. 99-4793, 2000 U.S. App. LEXIS 18665 (4th Cir. Aug. 3, 2000).

[58] *Id.* at *11–*12 ("While under certain circumstances, a person may have an expectation of privacy in content information, a person does not have an interest in account information

of privacy in the user information submitted to an ISP in the creation of an Internet account. Like the phone numbers in *Smith*, the court held that there was no reasonable expectation of privacy in information because it (1) did not disclose the content of any communication, and (2) was voluntarily disclosed to third parties.[59] This decision suggests that there is no reasonable expectation of privacy in addressing information, because it does not contain any "content" communication and is necessarily disclosed by the e-mail user to the ISP upon sending.

When viewed in isolation, the case law surrounding pen registers and trap and trace devices gives the appearance that e-mail addressing information will never be out of reach of Carnivore, for the FBI does not need a warrant in order to obtain it. Fortunately, Congress responded to concerns stemming from the *Smith* decision—that the FBI and other law enforcement agencies would be able to initiate pen registers without a judicial order—by passing the Electronic Communication Privacy Act (ECPA) of 1986.[60] Until Congress initiated legislation in the wake of the terrorist attacks of September 11, 2001, there was doubt as to whether the ECPA applied to the retrieval of Internet addressing and routing information.[61] Congress extinguished this doubt with passage of the

---

given to the ISP [Internet Service Provider] in order to establish the e-mail account, which is non-content information."); United States v. Kennedy, 81 F. Supp. 2d 1103, 1108–10 (D. Kan. 2000) (holding that the law enforcement's request and receipt of defendant's subscriber information from an ISP did not violate defendant's constitutional rights as he "has not demonstrated an objectively reasonable legitimate expectation of privacy in his subscriber info").

[59] *See Hambrick*, 2000 U.S. App. LEXIS 18665, at *7–*12.

[60] *See* United States v. Thompson, 936 F.2d 1249, 1251–52 (11th Cir. 1991) (generally describing how Congress sought to place limits on the government's ability to monitor electronic communications after the decision in *Smith*).

[61] *See* Electronic Privacy Information Center (EPIC), *Analysis of Provisions of the Proposed Anti-Terrorism Act of 2001 Affecting the Privacy of Communications and Personal Information, at* http://www.epic.org/privacy/terrorism/ata_analysis.html (Sep. 24, 2001) (noting that whether the pre-September 11th wiretap laws allowed the FBI to apply pen register/trap and trace provisions, which were couched in the language of telephone equipment, to electronic addressing and routing information "remains an open and debatable question"). For an illustration of Congress' view, in enacting the ECPA, that pen register/trap and trace devices applied only to telephone dialing information see the Senate report on the ECPA:

> Pen registers are devices that record the telephone numbers to which calls have been placed from a particular telephone. These capture no part of an actual telephone conversation, but merely the electronic switching signals that connect two telephones. The same holds true for trap and trace devices, which record the numbers of telephones from which calls have been placed to a particular telephone.

S. REP. NO. 99-541, at 10 (1986). *But see* COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2001), *available at* www.usdoj.gov/criminal/cybercrime/ searchmanual.htm (Jan. 2001) (interpreting the ECPA as

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, which extended the ECPA's definition of pen register/trap and trace devices to include technology intercepting "routing, addressing, and signaling information," but not the content of electronic communications.[62] Thus, so long as a government attorney presents an application to a court that "certifi[es] to the court that the information likely to be obtained . . . [by the pen register or trap and trace device] is relevant to an ongoing criminal investigation," the judge "*shall* enter an ex parte order authorizing the installation and use of a pen register or tap and trace device *anywhere in the United States*."[63] The changes to the pen register/trap and trace provisions of the ECPA provide considerably more protection to Internet users by, at a minimum, ensuring that law enforcement officers get a court order before instituting a pen register/trap and trace search. However, the pen register/trap and trace provisions exhibit a crucial weakness in that they apply a uniform "relevant to an ongoing investigation" threshold to addressing, routing, *and* telephone numbers, even though addressing and routing information reveal much more about an individual than does a telephone number.[64] The ECPA should ideally require a stronger showing for the interception of addressing and routing information as the interception of this data implicates privacy interests not present in the retrieval of telephone numbers.

According to the Independent Review of Carnivore, Carnivore can operate under a "pen mode" where it can gather, "TO and FROM e-mail addresses and the IP addresses[65] of computers involved" in file transfer and web browsing sessions.[66] Simply stated, Carnivore can be set to gather lists of the individuals a computer user has sent e-mail to and received e-mail from, lists of the computers

---

"permit[ing] law enforcement to obtain the addressing information of Internet e-mails . . . using a court order, just like it permits law enforcement to obtain addressing information for phone calls . . . .").

[62] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, §§ 216(c)(2)–(3), 115 Stat. 272.

[63] *Id.* § 216(b)(1) (emphasis added). This provision not only departs from the previous version of the statute by extending pen register/trap and trace rules to the interception of addressing and routing information, but also makes a court order valid nationwide. The ECPA originally provided that the order was good only "within the jurisdiction of the court." 18 U.S.C. § 3123(a) (1994). It goes without saying that this greatly enhances the Justice Department's ability to intercept addressing information out of the supervisory guise of the issuing judge.

[64] Butler, *supra* note 50, at A22.

[65] Each computer (including an individual's personal computer), website, and e-mail server has a unique IP address, which is part of the "global addressing system that allows people to find Web sites, e-mail to get to its intended recipients and computers on the Internet to communicate at all." Gary Chapman, *What's in a Web Domain Name? For a System Under Strain, It Spells Trouble*, L.A. TIMES, June 28, 2001, at T2.

[66] *Carnivore Independent Review*, *supra* note 3, at ix.

the user has transferred files with, and lists of computers/web-servers accessed by the user in the course of surfing the Internet. These types of addressing information reveal much more than a telephone number does. For instance, an e-mail address can indicate the specific identity of an individual someone communicates with, while a telephone number does not necessarily identify the individual.[67] E-mail addresses can also reveal the location, place of employment, and even the department that someone works in.[68]

Carnivore's ability to retrieve IP addresses has even greater potential for gathering personal information. The Carnivore Independent Review indicates that, while Carnivore can collect the source and destination IP addresses of computers a user accesses while web surfing or transmitting files, no "URL[69] and content of the target's web activities" are collected.[70] However, IP addresses reveal not only data about how information "transmitted over the network can be sent to its proper destination"[71] but also the websites an individual visits and their content.[72] Although Carnivore cannot retrieve website URL addresses during a pen register/trap and trace search, the FBI can use the information Carnivore obtains to view the content of websites. For example, intercepted IP addresses can be entered manually into a web browser to access a web site,[73] and once the name of the website is obtained, the FBI can use the website's URL to gain even more information about a user.[74]

---

[67] Bridis, *supra* note 50, at B9.

[68] JACOB PALME, ELECTRONIC MAIL 64 (1995) (describing how e-mails utilize domain addresses which split the address "into several subfields, department, company, street address, city, county, country, etc., each narrowing the field of potential recipients further").

[69] URL stands for "Universal Resource Locator" and is the address each of us type into a web browser when seeking to access a website. RICHARD SPINELLO, CYBER ETHICS: MORALITY AND LAW IN CYBERSPACE 154 (2000).

[70] *Carnivore Independent Review*, *supra* note 3, at 3-22.

[71] SPINELLO, *supra* note 69, at 154.

[72] Butler, *supra* note 50, at A22 (finding that "web addresses reveal not only that you visited Amazon.com, for example. They could also reveal what books you looked for or bought"). Other commentators have noted that IP addresses can reveal geographic information as well. LINCOLN STEIN, WEB SECURITY: A STEP-BY-STEP REFERENCE GUIDE 127 (1998) (noting that IP addresses can "give the remote site a strong hint of your geographic location or the company you work for").

[73] BOB LEVITUS & JEFF EVANS, WEBMASTER WINDOWS: HOW TO BUILD YOUR OWN WORLD WIDE WEB SERVER WITHOUT REALLY TRYING 37 (2d ed. 1997) (noting how IP numbers can be entered into web browsers to access websites in lieu of traditional web addresses). If a court were to find that retrieval of the websites an individual uses amounts to retrieval of content, then this would take searches of IP addresses out of the *Smith v. Maryland* pen register doctrine and into the *Katz* reasonable expectation of privacy analysis, possibly requiring the use of a warrant. *See supra* note 30 and accompanying text.

[74] *See* John Markoff, *Bitter Debate on Privacy Divides Two Experts*, N.Y. TIMES, Dec. 30, 1999, at C1 (explaining that some websites aggregate the Internet navigation patterns of their visitors to "learn about [the visitors'] shopping behavior" and that, consequently, web page addresses (URLs) "increasingly contain personal information the sites have gathered").

Though Carnivore is currently configured only to retrieve e-mail and IP addresses in "pen mode," the USA PATRIOT Act of 2001 permits pen register/trap and trace searches to recover *routing* information as well.[75] The interception of routing information poses an added threat to computer users' privacy interests as this information typically "shows the subject line of a message."[76] Thus, the FBI would be free to reconfigure Carnivore to conduct searches for routing information without any additional justification beyond the "relevant to an ongoing investigation" standard for pen register/trap and trace searches.

As has been demonstrated, e-mail addresses and IP addresses reveal considerably more information than phone numbers. However, the pen register/trap and trace provisions of the ECPA apply the same "relevant to an ongoing investigation" requirement for the interception of addressing, routing, *and* telephone numbers. Because of the greater privacy interests implicated with addressing and routing information, the ECPA needs to require a stronger justification from the FBI when it seeks to acquire this information with Carnivore. Although such a subtle oversight is understandable in light of the speed at which Congress enacted the USA PATRIOT Act in the wake of the September 11, 2001 terrorist attacks, the critical privacy interests at stake necessitates that Congress carefully reconsider this issue and apply different requirements for the interception of electronic addressing information.[77]

IV. THE PARTICULARITY REQUIREMENT

In addition to requiring warrants to search places (such as e-mail) where people have a reasonable expectation of privacy, the Fourth Amendment requires search warrants to "particularly describ[e] the place to be searched, and the persons or things to be seized."[78] The requirement of particularity in the warrant

---

[75] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 216(c)(2)–(3), 115 Stat. 272.

[76] Guy Guigliotta & Jonathan Krim, *Push for Increased Surveillance Powers Worries Some*, WASH. POST, Sept. 25, 2001, at A4.

[77] Proposals for revision of wiretap laws started circulating on Capitol Hill less than two weeks after the September 11 terrorist attacks. *See* John Lancaster & Jonathan Krim, *Ashcroft Presents Anti-Terrorism Plan to Congress; Lawmakers Promise Swift Action, Disagree on Extent of Measures*, WASH. POST, September 20, 2001, at A24. The final version of the Act was introduced in the House of Representatives on October 23, 2001; was passed by the House on October 24; was considered in *and* passed by the Senate on October 25; and was signed into law by President Bush on October 29. A mere seven days elapsed from the Act's introduction until its enactment. Bill Tracking Report, H.R. 3162 (LEXIS, Nexis Library, Legislation & Politics, U.S. Congress, Congressional Bills & Bill Tracking File).

[78] U.S. CONST. amend. IV. The requirement of particularity stems from the colonial times, where general or "rummaging" searches were conducted against colonists by royal revenue officers. Authorities were allowed with a warrant to enter a premises and search for anything

prevents the police from entering homes and rummaging through personal effects in order to find incriminating evidence and leaves nothing "to the discretion of the officer executing the warrant."[79] The Supreme Court's interpretation of the Fourth Amendment has indicated that the value in the particularity requirement lays in preventing "seizure of one thing under a warrant describing another."[80] Thus, police officers should have no discretion in choosing what to seize.[81] In theory, this too should provide adequate protection against the FBI's use of Carnivore to randomly search through e-mail messages. However, courts have not addressed the issue of particularity with regard to the interception of e-mail, and courts' lenient treatment of stored electronic communications searches indicate that agents will be left with much discretion in conducting Carnivore searches. Additionally, the FBI's intended procedures for operating Carnivore may lead to overbroad searches that turn up more materials than necessary.

There have been major issues developing with the application of the particularity requirement to searches of computer data, as incriminating data is often intermingled with non-incriminating, personal data.[82] The Supreme Court has recognized that there will be situations in which documents (or computer data) requested in a warrant will be intermingled with non-requested documents, and that this possibility mandates that law enforcement officials "take care to assure that [searches] are conducted in a manner that minimizes unwarranted intrusions upon privacy."[83] Unfortunately, in the context of stored data, many lower courts have interpreted search warrants requesting search and/or seizure of computer data to justify the search and/or seizure of *all* the materials on the computer regardless of their relevance to the commission of a crime. This has dramatic implications for Carnivore searches because, depending on how the FBI uses Carnivore, e-mails and Internet data not related to a crime listed in the warrant could be retrieved and searched by the FBI. Thus, the FBI could conceivably be allowed to collect e-mails transmitted from someone's account and then "rummage" through them to find incriminating materials.

The Tenth Circuit has had numerous occasions to consider whether authorities may search through multiple documents (including irrelevant ones) contained in a computer to obtain contraband listed in a warrant. A leading case on this issue is *United States v. Campos*,[84] where the court upheld the seizure of a defendant's entire computer system for purposes of locating images of child

---

that might be contraband. Under the particularity requirement, however, authorities must know what they are searching for *before* conducting the search and not after. *See* Boyd v. United States, 116 U.S. 616, 624 (1886).

[79] Marron v. United States, 275 U.S. 192, 196 (1927).

[80] Stanford v. Texas, 379 U.S. 476, 485 (1965).

[81] *Id.*

[82] *See* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J. L. & TECH. 75, 104 (1994).

[83] *Id.* (citing Andersen v. Maryland, 427 U.S. 463, 482 n.11 (1976)).

[84] 221 F.3d 1143 (10th Cir. 2000).

pornography. The defendant argued that search of his entire computer for pornography would constitute a "general search" in violation of the Fourth Amendment.[85] However, the court concluded that because the warrant authorized a focused search that looked only for "items relating to child pornography," search of the entire computer's contents was justified.[86] The court noted, however, that there are limitations on the authorities' ability to search through computer data, especially where the computer documents are so "intermingled" as to require "a more particularized inquiry."[87] The court then relied on its decision in *United States v. Carey*,[88] where it adopted the requirement that where documents are "so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents."[89]

The requirement of magistrate intervention in cases of "intermingled documents" was adopted from the Ninth Circuit's decision in *United States v. Tamura*.[90] In that case, the court found that the FBI had exercised too much discretion in a search of a corporation during a criminal investigation.[91] The warrant issued by the FBI authorized seizure of three specific types of documents; however, when the FBI agents discovered that it would take a long time to search through all of the documents, they requested that the company assist them in retrieving the documents.[92] The company refused to cooperate, and the FBI "seized 11 cardboard boxes of computer printouts, which were bound in 2000-page volumes; 34 file drawers of vouchers, also bound in 2000-page volumes; and 17 drawers of cancelled checks, which were bundled into files."[93] A significant portion of these records contained data not relevant to the crimes

---

[85] *Id.* at 1146.

[86] *Id.* at 1147. The court noted that:

> Computer storage devices . . . can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he often stores it in random order with deceptive file names. This requires searching authorities to *examine all the stored data* to determine whether it is included in the warrant.

Id. (emphasis added).

[87] *Id.* at 1148.

[88] 172 F.3d 1268 (10th Cir. 1999). *Carey* similarly dealt with a search of a computer system for contraband specified in a warrant. The warrant authorized a search for information relating to illegal drugs, but upon inspection of the computer, officers turned up child pornography. Analogizing a search of multiple computer files to be similar to searching for "intermingled documents" in a file cabinet, the court adopted procedures used by the Ninth Circuit in *Tamura v. United States*, 694 F.2d 591 (9th Cir. 1982). *Id.* at 1271.

[89] *Campos*, 221 F.3d at 1148 (citing *Carey*, 172 F.3d at 1275).

[90] 694 F.2d 591 (9th Cir. 1982).

[91] *Id.* at 594.

[92] *Id.*

[93] *Id.* at 594–95.

alleged in the warrant.[94] The court found that this type of "wholesale seizure . . . [was] 'the kind of investigatory dragnet that the fourth amendment was designed to prevent.'"[95]

The FBI justified its seizure and subsequent search of the documents on the grounds that the documents described in the warrant were intermingled with non-relevant documents, which made sorting difficult.[96] The court rejected this argument and held that where documents requested in a warrant are intermingled with irrelevant documents, "[t]he essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate."[97]

The requirement of magistrate intervention in the case of intermingled documents and computer files is an important step in ensuring that the FBI and other agencies do not have the authority to search through irrelevant, private documents when looking for materials as required in a warrant. However, though the court ultimately found that the government had exceeded the scope of the warrant, it refused to suppress any evidence obtained from the search. The court found that all the documents, which were eventually used in the case against the defendant, were lawful, because they had been "described in and therefore taken pursuant to the valid search warrant."[98] This is a crucial weakness of the decision, as it does not provide an adequate penalty (i.e., suppression of all the evidence that the FBI would have used in the case) to discourage law enforcement officials from reading through irrelevant, personal material when conducting a search.

Another critical weakness of the *Tamura* decision is that a large number of courts have simply refused to apply it to situations involving computer data. In *United States v. Scott-Emuakpor*,[99] the District Court for the Western District of Michigan upheld a warrant that provided for the seizure of "records, including computer files" related to the violation of immigration laws. The defendant argued that the files to be searched on the computer needed to be specified with more particularity, in order to avoid a general search through all of his private files.[100] The court, however, found that "in searching for such files, the agents had no way of knowing whether they would be found on computer hard drives or on

---

[94] *Id.*

[95] *Id.* (quoting United States v. Abrams, 615 F.2d 541, 543 (1st Cir. 1980)).

[96] *Id.*

[97] *Id.* at 596. The court suggested that law enforcement officers can avoid violations of suspects' Fourth Amendment rights by utilizing the procedures in the American Law Institute's Model Code of Pre-Arraignment Procedure. These procedures require officials to impound intermingled documents and inform the magistrate who initially issued the original warrant. The magistrate must then hold a hearing to allow any persons with an interest in the documents to move to have the documents returned or for "specification of such conditions and limitations on the further search for the documents to be seized as may be appropriate to prevent unnecessary or unreasonable invasion of privacy." *Id.* at 596 n.3.

[98] *Id.* at 596.

[99] 99-CR-138, 2000 U.S. Dist. LEXIS 3118 (W.D. Mich. Jan. 25, 2000).

[100] *Id.* at *16.

zip disks; nor did they know the format in which those files might be stored. Thus, the agents could not determine where those files were located without searching the files on both the hard drives and the zip disks."[101] Refusing to follow the decision in *Tamura*, the court distinguished it from the present case by reasoning that "*Tamura* did not involve computer files and therefore did not consider the specific problems associated with conducting a search for computerized records."[102] Ultimately, however, the court did suppress irrelevant information that exceeded the scope of the warrant, but it did not suppress all of the documents seized because the defendant had not demonstrated that the officers had a "flagrant disregard" for the search warrant's limits.[103]

The District Court for the Northern District of New York noted similar concerns with the seizing of computer data when it upheld a search of an America Online user's stored e-mails for evidence of pornography.[104] The court noted that while the language of the warrant[105] did not limit investigators to seizing only files containing images of child pornography, the FBI agents could not determine whether there was child pornography without seizing and searching all of the files.[106] Thus, it was not unreasonable to allow the FBI to take the data from the AOL accounts back to an FBI lab and search through the data for the incriminating materials specified in the warrant.[107]

---

[101] *Id.* at *17.

[102] *Id.* The court's decision is ultimately flawed, however, in reasoning that the search of computer files presents additional difficulties not present with the search of paper files. Both ultimately involve the same procedures, namely the search of the content of documents. Paper files, just like computer files, can be difficult to find and require sorting through irrelevant documents to get to the ones specified in the warrant. There would appear to be no reason why computer files should not be treated like "intermingled documents" in *Tamura* and require the intervention of a magistrate to ensure that privacy rights are not being unnecessarily trammeled. In fact, the danger of invasion of privacy is arguably greater with computers, as their storage capacity could potentially subject many times more private documents to the FBI's prying eyes under the *Scott-Emuakpor* rule.

[103] *Id.* at *25.

[104] United States v. Lamb, 945 F. Supp. 441 (N.D.N.Y. 1996).

[105] *See id.* at 458 (describing warrant as containing the broad statement seeking "all stored files in original format in individual files" in the defendant's account).

[106] *See id.* at 459 ("In these circumstances it is unreasonable to require the executing officers to identify which files actually contain child pornography and which do not in AOL's Virginia headquarters. That task may be more properly performed by a government computer technician at an FBI lab or office.").

[107] *Id.* Other cases have similarly held that authorities can search all the files contained in a computer for contraband. *See* United States v. Lacy, 119 F.3d 742, 746 (9th Cir. 1997) (holding that while the warrants described computer equipment in generic terms and "subjected it to blanket seizure . . . this type of generic classification is acceptable 'when a more precise description is not possible.'" A customs agent had stated that "there was no way to specify what hardware and software had to be seized to retrieve the images accurately."); *see also* United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (upholding warrant authorizing search of contents of computer, the court cited *Lacy* and found that *Tamura* could not apply in this case

The implications of these cases for the FBI's use of Carnivore are great. Despite the Fourth Amendment's requirement of particularity in searches, the FBI could conceivably conduct overbroad searches with Carnivore without any penalty from the courts. Thus, if the FBI specified in a warrant that it was seeking e-mails related to terrorist bombings, it could, either purposely or by a malfunction of Carnivore,[108] expand Carnivore's search criteria, intercept a wide-range of e-mails, and weed through the e-mails to determine which ones contained incriminating evidence. A broader search would be especially useful to the FBI where the search criteria may not reveal all of the desired information.[109] If a search turned up evidence of other crimes, that evidence would be suppressed, but other evidence relevant to the warrant would not be suppressed.[110] This gives the FBI little incentive to avoid overbroad searches and reduce unnecessary infringement into our privacy.

Aside from a court-imposed suppression incentive, the FBI's operating procedures as described in the Illinois Institute of Technology Research Institute's evaluation of Carnivore do not provide much assurance that the FBI agents using Carnivore will not employ overly broad search terms. Though a court order for an intercept with Carnivore must state "a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates," there is no judicial oversight of the search terms used to intercept e-mails.[111] After FBI agents obtain a warrant or an intercept order, they are free to exercise discretion in determining the search criteria to be used for retrieval of e-mail.

The only other form of oversight as to the particularity of the search criteria is the FBI's internal minimization procedures.[112] The first minimization technique is entering search criteria into Carnivore to ensure that only relevant e-mails are

---

because the government "had no way of knowing where the images were stored"); United States v. Hall, 142 F.3d 988, 996–97 (7th Cir. 1998) (finding that search warrants were sufficiently particular as they contained phrases limiting the scope of the search to documents and data containing child pornography).

[108] The comments on the *Carnivore System Technical Review* indicated that the Research Institute's tests of Carnivore lacked "analysis of operational and 'systems' issues, including interactions between the Carnivore code and its host environment and operating system. Many potential security flaws and *collection errors* are likely to be found in this area" (emphasis added). Bellovin et al., *supra* note 50. This observation tends to indicate that it is unclear whether or not a Carnivore search would intercept more information than requested. *See id.*

[109] This is similar to the situation that confronts us all when we use search engines on the Internet. Sometimes the search criteria do not yield enough information, thus necessitating the use of broader search criteria to retrieve more materials.

[110] *See* United States v. Tamura, 694 F.2d 591, 594–95 (9th Cir. 1982); United States v. Scott-Emuakpor, 99-CR-138, 2000 U.S. Dist. LEXIS 3118, at *25 (W.D. Mich. Jan. 25, 2000) (suppressing evidence obtained outside of the scope of the warrant, but refusing to suppress evidence relevant to the warrant).

[111] *Carnivore Independent Review*, *supra* note 3, at 3-1.

[112] *Id.* at 3-4.

intercepted.[113] This technique can be effective, assuming that Carnivore's interceptions do not turn up more information than requested. The Carnivore Independent Review concluded that "when Carnivore is used [correctly under a court] order, it provides investigators with no more information than is permitted by a given court order."[114] The report reviewing the findings of the Carnivore Independent Review, however, noted many flaws in the analysis of Carnivore's operation, which leave it far from clear as to whether Carnivore collects more information than necessary.[115] Specifically, the report noted that under a heavy collection load, Carnivore may not accurately collect data, and in pen mode (a mode where only addressing and signaling information are collected), there is the possibility that Carnivore may collect more packets than authorized.[116] The second minimization technique is used when FBI agents examine the collected e-mail packets with the special software designed to assemble the packets into whole e-mails. At that point, it is FBI policy for the agent to "determine[ ] which information is relevant and which is not."[117] Again, the FBI is left to its own devices to search for contraband through all of the intercepted material, even though it is not relevant to the search warrant. Taken together, the courts' inability to effectively apply the particularity requirement to searches of computer data and the lack of oversight over the FBI's use of search criteria when using Carnivore may allow the FBI to conduct overbroad searches of intercepted material, regardless of whether this material is relevant to a search warrant, thus constituting a significant intrusion into the privacy of individuals being searched.

V. CONGRESS STEPS IN: TITLE III AND THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

A. *Background*

The requirement of a warrant for interception of telephone and electronic communications is somewhat comforting, but Congress has repeatedly stepped into the picture to allow interception only "under carefully subscribed circumstances."[118] In response to the Supreme Court's decisions in *Katz* and *Berger*,[119] Congress passed the Omnibus Crime Control and Safe Streets Act of 1968 (hereinafter Title III).[120] This legislation imposed substantial restrictions on

---

[113] *Id.*

[114] *Id.* at xii.

[115] *See* Bellovin et al., *supra* note 50.

[116] *Id.*

[117] *Id.*

[118] S. REP. NO. 99-541, at 2 (1986).

[119] Katz v. United States, 389 U.S. 347 (1967) (extending Fourth Amendment protection to electronic interception of conversations); Berger v. New York, 388 U.S. 41 (1967) (same).

[120] S. REP. NO. 99-541, at 2 (1986). 18 U.S.C. §§ 2510–22 (1994) were first passed as Title III of the Omnibus Crime Control Act of 1968.

law enforcement's ability to intercept wire and oral communications. Title III largely continued in the same form until 1986, when Congress passed the Electronic Communications Privacy Act (hereinafter ECPA) to extend protection to "electronic communications,"[121] including electronic mail.[122] Though Title III as amended by the ECPA does provide some protection over intercepts of e-mail, the protections don't go nearly far enough to prevent abuse of Carnivore by the FBI. Title III's provisions for judicial supervision of the intercept process are inadequate to deal with the complexities of a search utilizing Carnivore. Additionally, as applied, Title III's requirement that the FBI minimize retrieval of unnecessary information has been broadly interpreted by the courts to allow a wide range of intrusive conduct.[123] Most glaringly, however, is Title III's lack of a suppression remedy to discourage FBI conduct in violation of its provisions.

1. *Requirements of the ECPA*

In order for an agency like the FBI to conduct an interception of e-mail with Carnivore, Title III as amended by the ECPA requires application for a wiretap order from a "Federal judge of competent jurisdiction"[124] supported by "probable cause."[125] The FBI can only make an application for a wire, oral, or electronic intercept pursuant to investigations of certain enumerated crimes.[126] A higher-

---

[121] As amended by the ECPA, Title III § 2510 defines "electronic communication" as

> any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—(A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

18 U.S.C. § 2510(12) (Supp. V 1999).

[122] *Id.* The Senate report indicates that Congress believed that the 1968 Act had become "hopelessly out of date" and had "not kept pace with the development of communications and computer technology." S. REP. NO. 99-541, at 2 (1986).

[123] *See* James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 77 (1997) (finding that "the minimization requirement . . . has not been strictly enforced by the judiciary").

[124] 18 U.S.C. § 2516(1) (Supp. V 1999).

[125] *See* 18 U.S.C. § 2518(3)(a)–(b) (1994) (requiring, *inter alia*, "probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense . . . [and] probable cause for belief that particular communications concerning that offense will be obtained through such interception").

[126] 18 U.S.C. § 2516(1)(a)–(e) (1994 and Supp. V 1999) (enumerating specific crimes for which interception of wire, oral, or electronic communications can be made, including sabotage of nuclear facilities or fuel; espionage; sabotage; piracy; offenses involving "murder, kidnapping, robbery, or extortion"; bribery; obstruction of criminal investigations; counterfeiting; and drug trafficking). The requirements for interception of electronic

level Justice Department official[127] must approve the application to the judge, and the judge may only grant the wiretap order if, based on the facts submitted by the applicant, there is a showing that probable cause exists and that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[128] The application also must include a provision that the intercept will be conducted "as soon as practicable" and that it will be "conducted in such a way as to minimize the interception" of irrelevant conversations.[129]

Title III also provides for limited judicial supervision to ensure that the interception is not taking too long, that the investigators are taking proper steps to minimize the interception of irrelevant conversations, and that the intercept is not proceeding beyond the bounds of the wiretap order.[130] Finally, the statute also provides for criminal and civil penalties for violation of its terms and for suppression of evidence received from unlawful oral and wire intercepts (but not electronic communications).[131]

---

communications, however, are more relaxed, and *any* federal felony will suffice to justify an application. 18 U.S.C. § 2516(3) (1994).

[127] *See* 18 U.S.C. § 2516(1) (Supp. IV 1998) (providing that "the Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge" for an order that authorizes interception of wire or oral communications).

[128] 18 U.S.C. § 2518(1)(a)–(d) (1994). Title III sets out the formal requirements of the application, requiring it to include, among others:

> (a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application; (b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been . . . committed . . . (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted; (c) a full and complete statement as to whether or not other investigative procedures have been tried and failed . . . (d) a statement of the period of time for which the interception is required to be maintained . . . .

18 U.S.C. § 2518(1) (1994).

[129] 18 U.S.C. § 2518(5) (1994).

[130] 18 U.S.C. § 2518(6) (1994) (providing that an order authorizing an intercept "*may* require reports to be made to the judge who issued the order showing what progress had been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge *may* require.") (emphasis added).

[131] 18 U.S.C. § 2511(4) (1994) (authorizing criminal penalties for unlawful interception and disclosure of wire, oral, or electronic communications); 18 U.S.C. § 2518(10)(a) (1994) (providing for suppression); 18 U.S.C. § 2520 (1994) (authorizing civil damages for violations).

B. *Judicial Supervision and the ECPA*

At the outset, it should be noted that many of the ECPA's shortcomings are due to the lack of judicial supervision over the intercept process. This lack of supervision makes it difficult for judges to adequately ascertain whether the FBI is properly minimizing its collection of communications, whether other investigative techniques could be utilized before resorting to an electronic intercept, or whether the surveillance itself is even necessary.[132] In its report evaluating Carnivore, the Illinois Institute of Technology Research Institute states that "[j]udges are involved in the Carnivore process throughout."[133] After issuing the order, according to the Carnivore Report, "the court often spot-checks minimization [and] ensures that the interception does not continue longer than is necessary."[134] While Title III does provide for progress reports to monitor minimization and the length of intercepts, the scope of the reporting provision does not provide for effective judicial supervision.[135] This is highlighted by the fact that the statutory language implementing progress reports is permissive in tone, and the judge's determination of the adequacy of reports is dependent entirely on the assertions of the officials filling out the reports.

The primary instrument for judicial supervision of electronic intercepts resides in section 2518(6) of Title III, which states that "[w]henever an order authorizing interception is entered pursuant to this chapter, the order *may* require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception."[136] Thus, judicial supervision is not even required for intercept orders, and appellate courts as a rule do not review the adequacy of progress reports or suppress evidence for failure of a judge to require progress reports.[137] Though most federal judges typically insist on reports issued at five-

---

[132] *See* 1 CLIFFORD S. FISHMAN AND ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING 13-5 (2d ed. 1995) (citing S. REP. NO. 90-1097 (1968), *reprinted* in 1968 U.S.C.C.A.N. 2112) ("Congress intended the progress report provision to provide a judicial 'check on the continuing need to conduct surveillance. At any time that the judge is convinced the need is no longer established, he or she may order the surveillance discontinued.'").

[133] *See Carnivore Independent Review*, *supra* note 3, at 3-6.

[134] *Id.*

[135] The FBI was more realistic about Title III's provisions regarding supervision in statements made before the House Judiciary Committee's Subcommittee on the Constitution, noting that "[j]udges may, and usually do, require periodic reports to the court . . . advising it of the progress of the interception effort." *See* Donald M. Kerr, *Statement for the Record of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation, on Internet and Data Interception Capabilities Developed by FBI Before the United States House of Representatives, The Committee on the Judiciary, Subcommittee on the Constitution, Washington, D.C., at* http://www.fbi.gov/ congress/congress00/kerr072400.htm (July 24, 2000).

[136] 18 U.S.C. § 2518(6) (1994) (emphasis added).

[137] *See* FISHMAN & MCKENNA, *supra* note 132, at 13-6 (citing United States v. Scafidi,

day intervals, state judges are less likely to require them.[138] Additionally, even if a judge requires a report, courts have "declined to impose sanctions when reports are submitted late or are not submitted at all."[139] The National Wiretap Commission, convened in 1976 to explore the abuses of traditional telephone taps, concluded:

> [U]nfortunately, "the protections to be enforced by the judiciary are often illusory." . . . Some courts have relied upon the issuing judge's supervision of monitoring to uphold total interception of all conversations even though the issuing judge was unaware that this practice was being followed. In such situations, judicial "supervision" may constitute little more than uninformed judicial ratification of improper conduct.[140]

The First Circuit's decision in *United States v. Charles*[141] illustrates the unwillingness of appellate courts to fault the judge's supervision of a wiretap, even when it is clearly insufficient to adequately ascertain whether the wiretap is being conducted properly. The court characterized as "pervasive" a judge's supervision of a wiretap based on the fact that: (1) the judge had reviewed the application for a wiretap supported by a fifty page affidavit by the police officer conducting the investigation; (2) the judge amended the wiretap order to include a minimization requirement after "carefully review[ing]" the wiretap application; and (3) the judge initially limited the wiretap to fifteen days.[142] Thus, according to the court, the supervision was sufficient even though there was no monitoring of the wiretap process beyond the initial application process.[143]

Even where a judge requires reports, they are usually insufficient to provide adequate supervision over the intercept activities. In *United States v. King*, the district court found that judicial supervision was sufficient where the report summarized the contents of the pertinent calls intercepted, as well as the number of calls intercepted, and the calls that were subjected to minimization procedures.[144] However, the investigating officers make such a report, thus the judge is forced to view the sufficiency of the wiretap procedures from the perspective of the law enforcement officers and not as a neutral observer. The

---

564 F.2d 633 (2d Cir. 1977)).

[138] *See id.* at 13-7 (citing NAT'L WIRETAP COMM'N REP. 96–97 (1976)).

[139] *Id.* at 13-6 (citing United States v. Canon, 404 F. Supp. 841, 847 (N.D. Ala. 1975)).

[140] *Id.* at 13-7 (citing HERMAN SCHWARTZ, TAPS, BUGS, AND FOOLING THE PEOPLE 23 (1977)).

[141] 213 F.3d 10, 23 (1st Cir. 2000).

[142] *Id.*

[143] *See id.*

[144] 991 F. Supp. 77, 91 (E.D.N.Y. 1998) (finding sufficient supervision where prosecutor and court supervised wiretaps through submission of ten-day reports to the court which "not only contain[ed] summaries of certain pertinent calls, but also detail[ed] the total calls intercepted . . . the number of calls actually completed, the number of calls over two minutes in length, and the number of calls minimized").

total dependence on police assertions in the reports raises a real possibility of police fabrication of reports. Because the only evidence as to the procedures followed for wiretaps would be in the hands of the law enforcement officials, this leaves criminal defendants with little or no chance to disprove the report's contents.[145]

The requirements of Title III thus make clear that, during a Carnivore search, there would be no judicial supervision of Carnivore to ensure that the FBI was complying with the intercept order. Even if the FBI was required to submit reports to the judge issuing the wiretap order, the judge would be totally dependent on the FBI's assertions in the report, making it easy for intercepts to simply not be reported or for the reports to be falsified. Also, proving that the FBI falsified or made misrepresentations on the report would be difficult, if not impossible. If a misrepresentation on a report was proven, some courts may be unable to offer any remedies.[146] Without adequate judicial supervision of Carnivore searches, there would be no assurance that the FBI has a continuing need to conduct a surveillance, or that they are using sufficient minimization procedures[147] to prevent over-collection of non-pertinent e-mails.

C. *The Minimization Requirement*

Another protection of Title III is the requirement that any intercepts of oral, wire, or electronic communications be minimized[148] in order to prevent

---

[145] Indeed, for the applications for wiretap orders (as opposed to the progress reports), the defendant bears a heavy burden of showing that the law enforcement officer's assertions in the initial application were falsified. *See* United States v. Crozzoli, 698 F. Supp. 430, 435 (E.D.N.Y. 1988) (citing Franks v. Delaware, 438 U.S. 154 (1978)). The defendant would have to "make a substantial preliminary showing that a false statement was knowingly and intentionally or with a reckless disregard for the truth made in the affidavit and that the statement was necessary to a finding of probable cause" in order to obtain a hearing on a matter. *Id.* This case suggests that a defendant would bear a similar heavy burden to prove that an officer's assertions in a progress report are false. *See also* United States v. Dorfman, 542 F. Supp. 345, 358 n.5 (N.D. Ill. 1982) (doubting whether it possessed authority to review progress reports and finding it "difficult if not impossible to determine whether misrepresentations in . . . reports are material," as they are not required under Title III); United States v. Harvey, 560 F. Supp. 1040, 1076 (S.D. Fla. 1982) (finding that defendant failed to prove that progress reports were falsified).

[146] *See Dorfman*, 542 F. Supp. at 358 n.5.

[147] *See infra* Part V.C. (describing minimization requirement).

[148] Minimization generally refers to law enforcement techniques used at the time of interception to limit the number of non-pertinent communications that are intercepted. There are many different types of minimization procedures that have been approved by the courts. FISHMAN & MCKENNA, *supra* note 132, at 14-5. One method is "intrinsic minimization," where law enforcement officials attempt to screen out non-pertinent material on the fly as the call is being intercepted. *Id.* Officers can accomplish this form of minimization by either (1) discontinuing monitoring of the call or (2) merely discontinuing the recording of the call. *Id.* at 14-5 to -6. Another method is "extrinsic minimization," which is accomplished by limiting

unnecessary intrusion on the privacy of individuals and ensure that communications seized are the ones stipulated in the court order.[149] As with other provisions of Title III and the ECPA, court interpretations of the minimization requirement have given law enforcement a great deal of leeway in determining what constitutes sufficient justification for not following minimization procedures. These interpretations open up the possibility that the FBI could use Carnivore to retrieve information unrelated to an investigation and unnecessarily intrude on individuals' privacy.

1. Scott v. United States

The Supreme Court established the standard for determining whether the minimization requirements of Title III were followed in *Scott v. United States*.[150] In *Scott*, the Court considered a challenge to a wiretap order issued pursuant to a narcotics conspiracy on the ground that the federal agents "failed to comply with the minimization requirement" in the order.[151] Emphasizing that the Fourth Amendment only prohibits unreasonable searches, the Court found that a determination as to whether proper minimization techniques were used depends on an objective "reasonableness" examination of the actions of the investigating officers in light of the circumstances surrounding the investigation.[152]

Factors that should be taken into account in determining the reasonableness of the minimization procedures include the circumstances surrounding the phone call and the circumstances surrounding the wiretap itself.[153] With respect to the circumstances surrounding the phone call, the Court found that the failure of investigators to use minimization techniques is justified in the case of short phone conversations, "one-time only calls," and "ambiguous" or "coded" conversations.[154] According to the Court, in these instances, the agents "can hardly be expected to know that the calls are not pertinent prior to their

---

monitoring to short periods of time (i.e., fifteen days as opposed to the statutory ceiling of thirty days). *Id.* at 14-6. "Dual recorder minimization" occurs when agents use two tape recorders to record conversations. For the first tape recording, agents make a "good-faith" effort to stop recording and listening when non-pertinent material comes up. *Id.* at 14-7. The second tape recording is made silently and is never reviewed, as it is only used to "rebut" any claim in court that minimization techniques were not used. *Id.* at 14-7. The final method utilized is "after the fact minimization," where entire conversations are recorded, but only pertinent portions are transcribed or re-recorded, while the remaining materials are sealed. *Id.* at 14-7 to -8.

[149] *See* 18 U.S.C. § 2518(5) (1994) (outlining requirement of minimization); United States v. Clemente, 482 F. Supp. 102, 109 (S.D.N.Y. 1979) (explaining that the purpose of minimization requirement is to prevent unnecessary intrusion on privacy); Dempsey, *supra* note 123, at 76.

[150] 436 U.S. 128 (1978).

[151] *Id.* at 132.

[152] *Id.* at 135–38.

[153] *Id.* at 140–41.

[154] *Id.* at 140.

termination."[155] The circumstances of the wiretap may also justify the non-use of minimization techniques. In the case of a conspiracy investigation, additional monitoring may be necessary to "determine the precise scope of the enterprise."[156] Also, during the initial phases of the investigation, the law enforcement officers may be justified in extensive monitoring in order to determine which types or categories of calls are non-pertinent and will not be intercepted in the future.[157]

Utilizing these factors, the Court then proceeded to reject the petitioner's claim that proper minimization techniques were not used. Though only forty percent of the calls were pertinent to the investigation, the Court found that the non-pertinent calls were short in duration, including calls to wrong numbers, calls where the other party did not answer, and "calls to the telephone company to hear the recorded weather message."[158] Additionally, the Court seized upon the fact that the investigation involved "a wide-ranging conspiracy."[159] Because of the many participants in the conspiracy, the Court concluded that even the most experienced officer would have difficulty determining the relevance of the calls.[160] Many of the calls were also what the Court deemed to be "one-time" calls: "Since these calls did not give the agents an opportunity to develop a category of innocent calls which should not have been intercepted, their interception cannot be viewed as a violation of the minimization requirement."[161]

2. *Minimization After* Scott

The Court's determination of what factors constitute "reasonableness" for the purposes of minimization requirements has been applied by lower courts to justify a variety of broad searches. [162] Most troubling has been lower courts' tendency to follow *Scott*'s directive that it is appropriate to listen to phone conversations without minimization to ascertain patterns of innocent calls for future "minimization."[163] One example of courts' willingness to allow extensive

---

[155] *Id.*

[156] *Id.*

[157] *Id.* at 141.

[158] *Id.* at 141–42.

[159] *Id.* at 142.

[160] *Id.*

[161] *Id.*

[162] *See* FISHMAN & MCKENNA, *supra* note 132, at 14-3. The authors state that while they recognize that many wiretaps involve complex investigations making determinations of relevance difficult, "some courts have been too willing to cite [the *Scott*] factors to excuse a failure to minimize without analyzing whether these factors were actually present to such an extent that minimization was completely impossible." *Id.*

[163] *Id.* at 14-13 (noting that "the practice of initial, total interception has a tendency to become self-perpetuating and self-justifying, and the minimization requirement has sometimes received little more than lip service"); *see* United States v. Quintana, 508 F.2d 867, 874 (7th Cir. 1975) (finding initial monitoring of calls to determine pattern of innocent conduct to be

monitoring without minimization occurred in *United States v. Cleveland*.[164] Like *Scott*, *Cleveland* involved a criminal defendant's challenge to a wiretap on minimization grounds. The court found an initial interception of 89.7% (pertinent and non-pertinent calls included) of the defendant's calls to be reasonable. The high percentage of interception was justified on the grounds that the government needed to listen to non-pertinent calls to determine the "identities of the suspected co-conspirators."[165]

Another result of the *Scott* decision is that courts have been willing to require no minimization for calls shorter than three minutes in duration. Thus, regardless of the pertinence of the calls, investigators are permitted to listen to and record all of the conversations resulting from the intercept. The *Cleveland* court determined that the minimization was reasonable after excluding all calls shorter than three minutes.[166] Other courts have been more restrictive, requiring calls to be under two minutes to be excused from the minimization requirement.[167] *Scott* has also resulted in a series of cases allowing investigators to listen to entire conversations because of the presence of "drug jargon." In *United States v. Williams*,[168] the Eighth Circuit Court of Appeals held that "more extensive wiretapping" is reasonable anytime agents "reasonably could have believed [that the intercepted conversations were] coded language referring to possible cocaine transactions."[169]

The result of these interpretations of the minimization requirement is that authorities can lawfully intercept a significant amount of irrelevant conversations. This constitutes a significant invasion of privacy rights and has serious implications to any e-mail users whose messages may fall prey to Carnivore's bite.[170] When applied to e-mail interceptions, judges and counsel may be left

---

"reasonable").

[164] 964 F. Supp. 1073, 1094 n.10 (E.D. La. 1997).

[165] *Id.* The court further reassured itself of the reasonableness of the intercept after considering the fact that, *not* including calls under three minutes in length and incomplete calls, 67% of the non-pertinent calls were subject to minimization procedures. *Id.* at 1094–95. Of course, this still meant that one-third of non-pertinent calls were being fully listened to by the investigators.

[166] *Id.* at 1094.

[167] United States v. Pichardo, 97 Cr. 233, 1999 U.S. Dist. LEXIS 13111, at *18 (S.D.N.Y. Aug. 24, 1999) (citing United States v. Capra, 501 F.2d 267, 275 (2d Cir. 1974)).

[168] 109 F.3d 502 (8th Cir. 1997).

[169] *Id.* at 507.

[170] The FBI argues that Carnivore was developed for the very purpose of minimizing non-pertinent e-mail interceptions. *See* Kerr, *supra* note 4. By allowing FBI agents to enter search terms relating only to the crime investigated, e-mails not pertaining to the crime will be left alone. *Id.* The problem with this is twofold. First, Carnivore has exhibited the potential to over-collect e-mail in test runs. *See supra* notes 50, 108. Second, the FBI has sole discretion to determine the search criteria used in conducting Carnivore searches. *See supra* note 13 and accompanying text. This, coupled with the fact that the actual Carnivore searches are unsupervised by the judiciary, can lead to collection of non-pertinent documents. *See supra* notes 132–40 and accompanying text.

scratching their heads and wondering what exactly will constitute "reasonable" minimization procedures. For example, does the two or three minute exception to the minimization requirement mean that FBI agents intercepting e-mails with Carnivore have free reign over short messages? If FBI agents can intercept e-mails in less than two minutes using Carnivore, are minimization requirements unnecessary? Under the drug jargon exception to the minimization requirement, it is conceivable that FBI agents could enter broad search criteria into Carnivore to pull up more e-mails, because the messages may be "ambiguous in nature or apparently involv[e] guarded or coded language."[171] Worse yet, under the *Scott* interpretation, full-blown searches of all of someone's e-mail with Carnivore might be justified as necessary "to establish categories of non-pertinent [e-mails] which will not be intercepted thereafter."[172]

In enacting the ECPA, Congress recognized that e-mail intercepts would require different procedures for minimization as "[i]t is impossible to 'listen' to a computer and determine when to stop listening and minimize as it is possible to do in listening to a telephone conversation."[173] The committee contemplated that minimization should be conducted by an initial investigator, who would delete all non-pertinent information before giving pertinent information to other investigators.[174] However, no federal court has considered the applicability of minimization procedures to the interception of e-mail, and whether the committee's proposed solution would be sufficient is uncertain. It must be noted that allowing an FBI agent to initially view all of the intercepted e-mails would not solve the problem of inadequate judicial supervision over the Carnivore search. Further, the congressional solution does not address the issue of whether some intercepts of e-mails presumptively do not require minimization, like the three-minute phone calls or initial intercepts. Thus, there are serious gaps in Title III's protections that Carnivore is poised to exploit and that will necessitate some form of legislative remedy to protect e-mail privacy.

D. *Electronic Communications = No Suppression*

The most glaring weakness in Title III and the ECPA's provisions is their failure to provide criminal defendants with a suppression remedy for the FBI's interception of electronic communications in violation of the statute. In any court proceeding, an "aggrieved person . . . may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom . . . ."[175] Nowhere in this section is there any mention of the

---

[171] Scott v. United States, 436 U.S. 128, 140 (1978).

[172] *Id.* at 141.

[173] FISHMAN & MCKENNA, *supra* note 132, at 14-38 to -39 (citing S. REP. NO. 99-541, at 31 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3585).

[174] *Id.* at 14-39.

[175] 18 U.S.C. § 2518(10)(a) (1994).

suppression of electronic communications. This omission on the part of Congress in enacting the ECPA was not accidental, as a suppression provision in an earlier version of the bill faced opposition from the Reagan Administration.[176] If a defendant wishes to suppress information obtained from an intercept conducted by Carnivore, the only remedies available are civil damages under the ECPA or suppression under the stricter constitutional standard.[177] The result is that the FBI is left without any real incentive to avoid sweeping Carnivore searches in violation of the ECPA. As Michael Leib notes, the lack of a statutory suppression rule "creates a situation in which law enforcement officials can be less vigilant in their application of [Title III] when electronic communication is involved."[178] Moreover, the lack of a suppression remedy is in conflict with Title III's purpose of discouraging "unlawful interception of wire and oral communication."[179] According to Leib, the same policy goal applies here, as "[u]sers of electronic communication have an interest in ensuring that the government be as diligent in applying the provisions of Title III when intercepting e-mail as when intercepting wire and oral communication."[180]

VI. LIKE A KID WITH A KEY TO UNLOCK ALL OF THE CANDY STORES: CAN WE TRUST THE FBI WITH CARNIVORE?

Under the existing statutory and constitutional framework that this note has described, a variety of searches that the FBI can conduct with Carnivore are entirely legal. However, the examination of the constitutional and statutory ramifications has assumed that the FBI will use Carnivore as it says it will. In Donald Kerr's statement to Congress regarding Carnivore's use, he states that "[i]n obedience of the law, the FBI obtains judicial authorization, in terms of *always* obtaining the appropriate court order required when intercepting wire and electronic communications' content or when acquiring addressing information and transactional record information . . . ."[181] But questions remain as to whether the FBI will use Carnivore legally and whether there is enough external supervision and internal restraint to prevent the FBI from searching our e-mail

---

[176] *See* Michael S. Leib, *E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communication to Title III's Statutory Exclusionary Rule and Expressly Reject a "Good Faith" Exception*, 34 HARV. J. ON LEGIS. 393, 410 (1997).

[177] United States v. Wells, IP 99-140-CR-B/F-02, 03, 06, 07, 09, 2000 U.S. Dist. LEXIS 12480, at *17 (S.D. Ind. Aug. 29, 2000) (citing S. REP. NO. 99-541, at 23 (1986)) ("In the event that there is a violation of law of a constitutional magnitude, the court involved in a subsequent trial will apply the existing Constitutional [sic] law with respect to the exclusionary rule."); *see* United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990) (noting the absence of a suppression remedy for electronic communication interceptions under the ECPA).

[178] Leib, *supra* note 176, at 418.

[179] *Id.*

[180] *Id.*

[181] Kerr, *supra* note 4 (emphasis added).

whenever it pleases.

One troubling scenario for Carnivore's abuse might be if the FBI uses it to "snoop" in order to discover whether users of e-mail are engaging in criminal or seemingly subversive activity. An FBI agent, under no supervision by any court or neutral third party, could conceivably enter broad search terms into Carnivore and intercept thousands of private e-mails. While the FBI claims that any evidence obtained through an illegal use of Carnivore would be suppressed in a court of law,[182] there is no judicial oversight preventing the FBI from using this evidence to seek out new leads in an investigation.[183] In the ensuing investigation, the FBI could then obtain judicial authorization for subsequent invasions of privacy.

This scenario is not far fetched, as it was suggested in a defendant's challenge to a court-ordered search of his computer system in *United States v. Kennedy*.[184] In *Kennedy*, the defendant was indicted for intentional receipt of child pornography.[185]The defendant had an account with a local Road Runner ISP, which he was using to download pictures.[186] Officials at the Road Runner headquarters received an anonymous call stating that the caller was at a friend's house and was using his Road Runner access to search through files located on the defendant's computer.[187] The officials at Road Runner searched the defendant's computer from a remote location, verified the caller's tip, and contacted the FBI.[188] Using this information, the FBI then executed a warrant to retrieve the defendant's account information and search defendant's home.[189] In a subsequent hearing, the defendant claimed that the evidence should be suppressed because it was obtained without a warrant.[190] Specifically, he claimed that the search performed by the anonymous caller was by a government actor and therefore required a warrant.[191] Because the defendant did not establish that the anonymous caller was a government agent,[192] the court rejected the defendant's claim, noting that the "Fourth Amendment's protection against unreasonable

---

[182] *Id.*

[183] The FBI's assertion that any evidence obtained in violation of the ECPA would be suppressed is suspect, as the provisions of the ECPA do not have an exclusionary remedy for violation of its provisions. 18 U.S.C. § 2518 (1994); *see* United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (concluding that even if information was turned over to authorities pursuant to an inadequate court order in violation of the ECPA, the statute "speaks nothing about the suppression of information in a court proceeding").

[184] *Kennedy*, 81 F. Supp. 2d at 1112.

[185] *Id.* at 1105.

[186] *Id.* at 1106.

[187] *Id.* at 1106–07.

[188] *Id.*

[189] *Id.* at 1107–08.

[190] *Id.* at 1112.

[191] *Id.*

[192] *Id.*

searches and seizures 'proscribes only governmental action; it is wholly inapplicable "to a search or seizure, even an unreasonable one, effected by a private individual."'"[193]

Kennedy thus indicates how easy it would be for the FBI to surreptitiously use Carnivore to find incriminating evidence, use a phony phone call as an "anonymous caller" to report the incident to the ISP, and then wait for the ISP to report the incident to the FBI. Using the information provided by the ISP, the FBI could then execute further valid warrants. Though the *Kennedy* court claimed that the defendant had not met the burden of establishing that the anonymous caller was an FBI agent, this evidence would be virtually impossible for *any* criminal defendant to put forward.

A response to these fears is that the FBI can be trusted to not exceed the bounds of the law and to use Carnivore properly. However, the past history of the FBI, as well as recent instances of its abuse of the justice system, indicate that the FBI cannot be trusted to monitor Carnivore itself and must be subject to some neutral oversight. During the reign of Director J. Edgar Hoover, the FBI was notorious for exceeding the bounds of citizens' privacy rights. For example, Director Hoover personally authorized "a series of break-ins and allegedly illegal wiretaps" during investigations of the families and friends of Weather Underground fugitives.[194] Though the FBI's excesses have lessened since that time, there have been many recent instances of the FBI overstepping its authority. One such example was the FBI's program of targeting Arab-Americans for interviews regarding terrorism in 1991.[195] Another example was the scandal that plagued the FBI's operation of its crime lab in 1997. In a report, the Inspector General at the time, Michael Bromwich, reported that agents at the lab gave "scientifically flawed and inaccurate testimony" in court, and that the agents made "errors that repeatedly favored prosecution cases."[196] These instances of misconduct by the FBI demonstrate that unsupervised use of Carnivore could easily lead to abuse. In the end, judicial supervision of the FBI's use of Carnivore will be necessary to prevent the Orwellian situation of *1984*—where everyone's thoughts and writings are being probed by an overbearing, omnipotent, and intrusive federal government.

VII. CONCLUSION: CONGRESS SHOULD MUZZLE CARNIVORE

As the Supreme Court aptly noted in *Berger v. New York*, "[f]ew threats to liberty exist which are greater than that posed by the use of eavesdropping

---

[193] *Id.* (quoting United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

[194] Timothy S. Robinson, *Testimony Cites Hoover Approval of Black-Bag Jobs*, WASH. POST, July 13, 1978, at A4.

[195] *The F.B.I. Is Calling*, N.Y. TIMES, Jan. 29, 1991, at A20.

[196] *Inspector Criticizes FBI Crime Lab*, ST. LOUIS POST-DISPATCH, Apr. 16, 1997, at 4A.

devices."[197] Carnivore is a powerful tool at the FBI's disposal. With it, not only can federal agents search anyone's e-mail messages from the comfort of their own office, but they can potentially monitor someone's Internet usage as well.[198] The problems with Carnivore are clear: There are too many possibilities that Carnivore will intercept more e-mail than necessary, too few protections imposed by federal constitutional and statutory law, and an outright absence of sufficient judicial supervision of the FBI.

A. *What Should Be Done?*

The solution to many of the issues posed by Carnivore lies in the hands of Congress. Short of banning the use of Carnivore, Congress has the ability to enhance the Title III and ECPA protections and ensure that the FBI does not have too much discretion in conducting e-mail intercepts. The Internet was in its infancy when the ECPA was passed in 1986, and Internet usage, as well as technology for intercepting Internet information like Carnivore, has since soared.[199] An amendment to the ECPA must respond to the changing nature of the Internet and its steadily increasing popularity.

To that end, Congress should start by extending the statutory suppression remedy to include electronic intercepts. This is what is currently done for oral and wire intercepts, and public policy dictates that it should be done for electronic intercepts as well.[200] Without a suppression remedy, the FBI has no real incentive to ensure that they are following the protections Congress established with Title III and the ECPA. Knowing that their investigations will be in jeopardy if the provisions of Title III are not followed, investigators will be forced to use reasonable procedures to minimize the interception of non-pertinent communications and to ensure that the scope of the wiretaps does not go beyond the requirements of the wiretap order. Additionally, Congress should establish a regime under which electronic communication intercepts are monitored by a neutral and detached magistrate. It is insufficient for judges to conduct their monitoring on the basis of progress reports made up by the same people (i.e., FBI agents) who are trying to maintain and preserve the intercept operation.[201] A judicial oversight regime where a representative of the judiciary would conduct

---

[197] Berger v. New York, 388 U.S. 41, 63 (1967).

[198] *See Carnivore Independent Review*, *supra* note 3, at xiii (noting that Carnivore can monitor HTTP files retrieved by a target individual).

[199] *See* Dempsey, *supra* note 123, at 80–82 (noting that when the ECPA was enacted in 1986 only 50,000 computers were hooked to the Internet, but by 1996 that number had increased to over 9.4 million with 40 million people worldwide utilizing the Internet and noting that "[e]-mail is in some respects easier to intercept than regular mail," and to that end, law enforcement officials have taken advantage of this weakness and developed new technologies for interception).

[200] *See* Leib, *supra* note 176 and accompanying text.

[201] *See supra* notes 144–45 and accompanying text.

minimization and/or observe the use of Carnivore would be a reasonable means to ensure that the public's rights under the Fourth Amendment and Title III are protected. Indeed, the Tenth Circuit in *Tamura* ratified a similar regime of judicial oversight.[202] Congress should also close the gaps in the minimization requirement and require a higher showing of necessity when officers seek to justify non-minimized interception of e-mail. Additionally, a complete ban on the ability of law enforcement officials to seize non-relevant e-mail at the beginning of the investigation for the purpose of identifying patterns of criminal activity should be considered.

With regard to pen registers, Congress should amend the ECPA to require an increased justification for judicial orders authorizing the interception of routing and addressing information in light of the fact that this data can reveal extensive information about an Internet user. Because Internet addressing and routing information reveals far more information than telephone numbers (to which pen registers and trap and trace devices were originally applied), it is necessary for Congress to increase the required justification for a pen/ trap order to mirror the probable cause requirement used in traditional wiretap orders.[203]

Finally, in light of the revelations that it has not yet been determined whether or not Carnivore can safely conduct searches without over-collection of non-pertinent e-mails, it may be wise for Congress to consider new policies surrounding implementation of such search devices by the FBI.[204] For example, when should an electronic communication interception device be cleared for full-time law enforcement use? Unlike the FBI's current implementation of Carnivore, it should be necessary for the FBI to seek review of Carnivore's operation through an independent testing process to evaluate its integrity.[205]

---

[202] *See* United States v. Tamura, 694 F.2d 591, 596 (9th Cir. 1982) (requiring impoundment of seized documents and subsequent intervention of a magistrate where documents are intermingled making separation of relevant versus irrelevant documents difficult).

[203] *See* 18 U.S.C. § 2518(3) (1994) (requiring probable cause for wiretap order); Bellovin, *supra* note 50 and accompanying text (noting "potential over-collection in pen mode").

[204] *Id.*; *see* Kevin Poulsen, *Report: Carnivore Needs Work*, SECURITYFOCUS NEWS, *at* http://www.securityfocus.com (Nov. 22, 2000).

[205] *See id.* (noting criticisms that review of Carnivore by the Illinois Institute of Technology Research Institute had "ties to the Clinton administration").